УДК 343

ПРОЦЕССУАЛЬНЫЙ ПОРЯДОК ОБНАРУЖЕНИЯ, ФИКСАЦИИ И ИЗЪЯТИЯ ЦИФРОВЫХ СЛЕДОВ

Астахова Д.А.[1]

Студент Института истории и права

Калужский государственный университет им. К. Э. Циолковского

Калуга, Россия

Аннотация

В статье рассматриваются теоретические и практические вопросы использования цифровых следов в уголовном судопроизводстве. Проанализированы понятие и сущность цифровых следов, особенности их обнаружения, фиксации и изъятия с учетом положений уголовно-процессуального законодательства и иных нормативных правовых актов. Сделан вывод о возрастающем значении цифровой информации в процессе расследования преступлений и необходимости соблюдения специальных процессуальных требований при работе с цифровыми следами.

Ключевые слова: цифровые следы, уголовный процесс, порядок обнаружения, изъятие данных, электронные доказательства, компьютерная информация.

[1] *Научный руководитель: Ильяш А.В., Заведующий кафедры Юриспруденции, к.ю.н., Калужский государственный университет им. К. Э. Циолковского, Калуга, Россия*
Scientific adviser: Ilyash A.V., Head of the Department of Jurisprudence, Candidate of Law, Kaluga State University named after K. E. Tsiolkovsky, Kaluga, Russia

PROCEDURAL REGIMEN OF DETECTION, FIXATION AND SEIZURE OF DIGITAL TRACES

Astakhova D.A.

Student of the Institute of History and Law

Kaluga State University named after K. E. Tsiolkovsky

Kaluga, Russia

Abstract

The article discusses the theoretical and practical issues of using digital traces in criminal proceedings. The concept and essence of digital traces, the features of their detection, fixation and seizure, taking into account the provisions of criminal procedure legislation and other regulatory legal acts, are analyzed. The conclusion is made about the increasing importance of digital information in the process of crime investigation and the need to comply with special procedural requirements when working with digital traces.

Keywords: digital traces, criminal proceedings, detection procedures, data seizure, electronic evidence, computer information

В современных условиях стремительной цифровизации общественных отношений информационные технологии активно проникают во все сферы жизнедеятельности, включая преступную деятельность и способы сокрытия ее следов. В связи с этим особую значимость приобретает исследование вопросов, связанных с цифровыми следами в рамках уголовного судопроизводства. Практика расследования преступлений показывает, что электронные устройства, сетевые ресурсы, цифровые носители информации и иные информационные

системы всё чаще выступают источниками доказательственной информации. Вместе с тем развитие цифровой среды опережает совершенствование уголовно-процессуального регулирования, что приводит к определенным проблемам как в теории, так и в правоприменительной практике. Актуальность выбранной темы обусловлена необходимостью теоретического осмысления юридической сущности и процессуального порядка обнаружения, фиксации и изъятия цифровых следов. Объектом исследования являются общественные отношения, возникающие в сфере использования цифровых следов в уголовном процессе, а предметом – нормы УПК РФ и их применение в данной области.

В современной юридической науке существуют различные подходы к понятию «цифровые следы». Например, группа криминалистов (А. М. Багмет, В. В. Бычков, Н. Н. Ильин, С. Ю. Скобелин) считает, что «цифровой след – это любая криминалистически значимая компьютерная информация, т. е. сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» [6, 7]. По мнению А.Б. Смушкина, «виртуальные следы» представляют собой следы совершения любых действий (включения, создания, открывания, активации, внесения изменений, удаления) в информационном пространстве компьютерных и иных цифровых устройств, их систем и сетей» [8]. Как отмечает С. С. Минаков, «к особенностям цифровых следов можно отнести двойственную природу информационно-компьютерных объектов, которая включает информационно-цифровую и материальную составляющие» [7, 63].

На основе данных высказываний можно сделать вывод, что цифровые следы сочетают в себе как материальные аспекты, которые проявляются в виде данных и информации, хранящихся на цифровых носителях, так и идеальные аспекты, выражающиеся в значениях и контекстах, которые эти данные приобретают в процессе их использования и интерпретации. Тем самым сущность цифровых следов заключается не только в их информационной

природе, но и в особом механизме следообразования, который происходит в электронной среде и требует применения специальных криминалистических знаний для их обнаружения, исследования и последующего использования в доказывании.

Обнаружение цифровых следов в уголовном судопроизводстве представляет собой первоначальный и один из наиболее значимых этапов работы с электронной доказательственной информацией, поскольку именно на данной стадии определяется возможность дальнейшего процессуального использования соответствующих сведений. Действующее уголовно-процессуальное законодательство Российской Федерации не содержит самостоятельного определения цифровых следов, однако процессуальный порядок их обнаружения вытекает из общих положений о собирании доказательств и производстве следственных действий. Так, в соответствии со ст. 86 УПК РФ собирание доказательств осуществляется дознавателем, следователем, прокурором и судом путем производства следственных и иных процессуальных действий [1]. На практике обнаружение цифровых следов наиболее часто осуществляется в ходе осмотра места происшествия (ст. 176 -177 УПК РФ), а также при осмотре предметов и документов, включая электронные носители информации (ст. 81, 84 УПК РФ). Особое значение имеет соблюдение процессуальной формы, поскольку нарушение установленного законом порядка получения цифровой информации может повлечь признание соответствующих доказательств недопустимыми в силу ст. 75 УПК РФ.

Кроме того, в системе мер по обнаружению цифровой информации предусмотрена ст. 186.1 УПК РФ [1]. Данная норма устанавливает порядок получения информации о соединениях между абонентами и абонентскими устройствами. В отличие от традиционных следственных действий, здесь обнаружение следов происходит опосредованно – через взаимодействие с операторами связи. Порядок обнаружения следов в электронной переписке

детализируется в ст. 185 УПК РФ. Наложение ареста на почтово-телеграфные отправления, их осмотр и выемка в контексте цифровых технологий охватывают не только традиционные письма, но и электронную корреспонденцию, передаваемую через провайдеров. В научной литературе подчеркивается, что сложность реализации данных норм заключается в необходимости получения судебного решения, что зачастую вступает в противоречие с требованием оперативности при расследовании киберпреступлений.

Наряду с уголовно-процессуальными механизмами важную роль в выявлении цифровых следов играют оперативно-розыскные мероприятия. В соответствии со ст. 6 Федерального закона «Об оперативно-розыскной деятельности» к таким мероприятиям относятся, в частности, наблюдение, получение компьютерной информации, обследование помещений, зданий, сооружений, участков местности и транспортных средств, а также снятие информации с технических каналов связи [2]. Указанные меры позволяют выявить цифровые следы еще до возбуждения уголовного дела либо на начальном этапе расследования, обеспечивая своевременное обнаружение электронных данных, имеющих доказательственное значение.

Следователь, определяя место осмотра, должен акцентировать внимание на местах вероятного нахождения электронных носителей информации. Помимо определения координат места осмотра, обязательным элементом подготовки является получение информации о месте. Например, проведение осмотра мобильного телефона вблизи предметов, обладающих сильным электромагнитным излучением, может привести к уничтожению компьютерной информации. Таким образом, готовясь к осмотру, следователю необходимо собрать данные о наличии объектов, оборудования, аппаратуры, устройств, обладающих сильным электромагнитным излучением, на месте предполагаемого осмотра (например, путем опроса представителей организации, подлежащей осмотру) [9, 9].

Фиксация доказательства, в том числе находящегося в виде компьютерной информации, преследует цель запечатления фактических данных. Причем, если на первый план в процессуальном понимании фиксации таких доказательств выступает процессуальная форма их удостоверения и запечатления, то с криминалистических позиций понятие фиксации доказательственной компьютерной информации носит содержательный характер [10, 85].

В соответствии со ст. 74 УПК РФ доказательствами по уголовному делу признаются любые сведения, на основе которых устанавливаются обстоятельства, имеющие значение для уголовного дела [1]. При этом применительно к цифровым следам такие сведения могут содержаться в протоколах следственных действий, заключениях экспертов, вещественных доказательствах, а также иных документах, содержащих электронную информацию. Положения статей 164, 166 и 167 УПК РФ определяют общие правила производства следственных действий и требования к составлению протокола, который является основным процессуальным средством фиксации цифровых следов. В нём должны быть подробно отражены технические характеристики обнаруженного устройства, условия его обнаружения, последовательность действий следователя, примененные технические средства, а также сведения о лицах, участвовавших в производстве следственного действия. Особенность фиксации цифровых следов состоит в необходимости использования специальных криминалистических и технических методов. В этой связи существенное значение имеет участие специалиста, предусмотренное ст. 58 УПК РФ. Специалист оказывает содействие следователю в выявлении, закреплении и копировании электронной информации, а также консультирует по вопросам безопасного обращения с цифровыми носителями.

Дополнительные организационные ориентиры содержатся в Приказе Следственного комитета РФ от 08.08.2013 № 53 «Об организации работы следователей-криминалистов в Следственном комитете Российской Федерации».

Указанный акт закрепляет обязанность следователей-криминалистов обеспечивать криминалистическое сопровождение расследования, применять научно-технические средства, а также участвовать в обнаружении и закреплении следов, имеющих доказательственное значение [3]. В современных условиях данные положения распространяются и на цифровые следы как разновидность криминалистически значимой информации.

Процессуальный порядок изъятия цифровых следов и их материальных носителей в ходе досудебного производства выступает завершающим этапом собирания доказательств, непосредственно затрагивающим конституционные права участников уголовного судопроизводства на неприкосновенность собственности и частной жизни. В силу положений уголовно-процессуального закона, изъятие электронных данных и технических устройств производится главным образом в рамках таких следственных действий, как обыск (ст. 182 УПК РФ) и выемка (ст. 183 УПК РФ) [1]. При этом ключевым условием правомерности данных процедур является соблюдение императивных требований, закрепленных в ст. 164.1 УПК РФ.

Статья 164.1 УПК РФ устанавливает специальный режим, согласно которому не допускается изъятие электронных носителей информации, если это может привести к необоснованному прекращению или приостановлению законной деятельности юридических лиц или индивидуальных предпринимателей за исключением трёх случаев: вынесение постановления о назначении судебной экспертизы, наличие прямого судебного решения либо ситуации, когда на носителях содержится незаконная информация или существует риск ее утраты при копировании [1]. В ч. 2 ст. 164.1 УПК РФ предусмотрено, что изъятие должно проходить с обязательным участием специалиста, а по ходатайству законного владельца специалистом осуществляется копирование информации на предоставленные владельцем носители. Данный подход соотносится с положениями Федерального закона «Об

информации, информационных технологиях и о защите информации», который закрепляет принцип защиты информации от неправомерного доступа, уничтожения, модификации и её распространения [4].

Также существенное значение для понимания правовой природы изъятия и копирования компьютерных данных имеют разъяснения, содержащиеся в Постановлении Пленума Верховного Суда РФ от 15.12.2022 № 37 [5]. В пункте 4 данного Пленума установлено, что под копированием компьютерной информации понимается перенос имеющейся информации на другой электронный носитель при сохранении неизменной первоначальной информации либо ее воспроизведение в материальной форме. Такое толкование подчеркивает, что при процессуальном изъятии путем копирования по правилам ст. 164.1 УПК РФ юридически значимая сущность цифрового следа не утрачивается и не видоизменяется.

В результате проведённого исследования можно сделать вывод о том, что цифровые следы в современных условиях приобретают всё большее значение для расследования преступлений. Развитие информационных технологий и широкое использование сети «Интернет» приводят к тому, что значительная часть преступной деятельности оставляет именно цифровые следы, которые могут выступать важными доказательствами по уголовному делу.

В ходе работы были рассмотрены понятие и сущность цифровых следов, особенности их обнаружения, фиксации и изъятия. Анализ норм уголовно-процессуального законодательства показал, что работа с цифровой информацией требует соблюдения специальных процессуальных и технических правил, поскольку электронные данные легко изменить или уничтожить. Таким образом, эффективность расследования преступлений в сфере информационных технологий напрямую зависит от правильности обращения с цифровыми следами и соблюдения требований закона при их получении и закреплении.

Библиографический список

1. "Уголовно-процессуальный кодекс Российской Федерации" от 18.12.2001 N 174-ФЗ (действующая редакция). Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_34481/ // (дата обращения: 02.05.2026). – Текст электронный.
2. Федеральный закон "Об оперативно-розыскной деятельности" от 12.08.1995 N 144-ФЗ (действующая редакция). Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_7519/ // (дата обращения: 02.05.2026). – Текст электронный.
3. Приказ СК России от 08.08.2013 N 53 "Об организации работы следователей-криминалистов в Следственном комитете Российской Федерации" (действующая редакция). Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_219616/ // (дата обращения: 17.05.2026). – Текст электронный.
4. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (действующая редакция). Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61798/ // (дата обращения: 18.05.2026). – Текст электронный.
5. Постановление Пленума Верховного Суда РФ от 15.12.2022 N 37 "О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет" (действующая редакция). Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_434573/ // (дата обращения: 18.05.2026). – Текст электронный.
6. Багмет, А. М. Цифровые следы преступлений: монография / А. М. Багмет, В. В. Бычков, С. Ю. Скобелин, Н. Н. Ильин. - Москва: Проспект, 2021. - 168 с. - ISBN 978-5-392-32868-0. - Текст: электронный // ЭБС "Консультант

студента»:[сайт].-URL: https://www.studentlibrary.ru/book/ISBN9785392328680.html (дата обращения: 03.05.2026). - Режим доступа: по подписке.

7. Минаков, С. С. Информационные технологии и преступления : учеб. пособие / С. С. Минаков, П. В. Закляков. - Москва: ДМК Пресс, 2023. - 160 с. - ISBN 978-5-93700-194-8. - Текст: электронный // ЭБС "Консультант студента»:[сайт].-URL: https://www.studentlibrary.ru/book/ISBN9785937001948.html (дата обращения: 03.05.2026). - Режим доступа: по подписке.
8. Смушкин, А. Б. Виртуальные следы в криминалистике / А. Б. Смушкин // Законность. – 2012. – № 8(934). – С. 43-45. – EDN PBJDJH.
9. Тактика следственных действий, направленных на отыскание, обнаружение, изъятие и исследование электронных носителей и информации на них: учебное пособие / А. А. Кузнецов, Д. В. Муленков, С. В. Пропастин, А. Б. Соколов. — Омск: Омская академия МВД России, 2015. — 116 с. — ISBN 978-5-88651-605-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/61786.html (дата обращения: 10.05.2026). — Режим доступа: для авторизир. пользователей
10. Электронные доказательства в уголовном судопроизводстве: учебник для вузов / ответственный редактор С. В. Зуев. — Москва: Издательство Юрайт, 2025. — 193 с. — (Высшее образование). — ISBN 978-5-534-13286-1. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567334 (дата обращения: 18.05.2026).